

Der Auslandsüberwachung wird (fast) alles möglich gemacht – zur Reform des Bundesnachrichtendienstgesetzes (BNDG)

Gastautor

2016-07-05T11:49:24

von [ANNELIE SIEMSEN](#)



Die

Enthüllungen Edward Snowdens ziehen weiterhin Kreise – im Zuge einer „Reform“ der nachrichtendienstlichen Überwachung verabschiedete die Große Koalition im Juni einen Gesetzentwurf zur „Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes“. Doch anstelle sich ernsthaft mit den Herausforderungen der digitalen und automatisierten Überwachung auseinanderzusetzen, werden die als verfassungswidrig kritisierten Praktiken entweder so weit wie möglich in Gesetzesform gegossen und einfach ignoriert. Außer Acht gelassen wurde auch das im April ergangene Urteil des Bundesverfassungsgerichts zum Schutz personenbezogener Daten.

Status quo

Die Überwachung durch Nachrichtendienste wird von der Telekommunikationsfreiheit aus Art. 10 GG erfasst. Bei der Erhebung einzelner personenbezogener Daten spielt das Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG eine Rolle. Die Bindung aller Staatsgewalt an die Grundrechte gilt im Grundsatz auch für Auslandssachverhalte und nichtdeutsche Staatsbürger, wobei die Grundrechtsgeltung entsprechend der Besonderheiten des jeweiligen Auslandssachverhalts modifiziert werden. Nach der bisherigen Gesetzeslage darf der BND offene und verdeckte Maßnahmen zur Erhebung personenbezogener Daten (§§ 2 und 3 Bundesnachrichtendienstgesetz [BNDG] i.V.m. § 8 Abs. 2 Bundesverfassungsschutzgesetz [BVerfSchG]) sowie

einzelne und massenhafte Erfassung von Telekommunikationsdaten (§§ 3 und 5 Artikel 10-Gesetz) vornehmen. Dies ist ihm innerhalb der ganzen Bandbreite seiner Aufgabenstellung, die in der Aufklärung von Gefahren aus dem Ausland besteht, erlaubt.

Soweit er außerhalb des deutschen Staatsgebiets agiert, sieht sich der BND unter Heranziehung fragwürdiger Theorien wie der „Weltraumtheorie“ und der „Theorie des virtuellen Auslands“ nicht an das BNDG gebunden (mehr [hier](#)). Doch auch wenn jedenfalls diese Theorien rechtlich nicht haltbar sind, so erlaubt § 5 Abs. 2 Satz 3 Artikel 10-Gesetz gleichwohl weitergehende Eingriffe in die Kommunikation nichtdeutscher Staatsbürger im Ausland. Im Prinzip sind den Datenverarbeitungen im Ausland kaum Grenzen gesetzt und auch die Kontrolle der Praktiken kann nur sehr eingeschränkt erfolgen. Die für den BND zuständige Datenschutzbeauftragte [erklärte](#), dass sie ohne die Mitwirkung des BND kaum Kontrollen vornehmen könne. Ein aus grundrechtlicher Perspektive weiterer problematischer Aspekt an der derzeitigen Überwachungspraxis ist, dass vermutet werden muss, dass Daten im sog. Ring-Tausch mit anderen ausländischen Geheimdiensten übertragen werden, wodurch der hierzulande geltende Grundrechtsschutz umgangen wird (mehr [hier](#) und [hier](#)).

Der Gesetzentwurf zur „Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes“ nimmt Stellung zu diesen Bedenken – nur um sie dann zu verschärfen.

„Reform“

So wird zwar ausdrücklich klargestellt, dass das Gesetz auch für Auslandssachverhalte gilt („*Erhebung von (...) Daten aus internationalen Telekommunikationsnetzen*“) – solange die Erhebung vom Inland aus stattfindet. Damit bleibt aber für die reine Auslandstätigkeit das bisherige Problem bestehen: Erfolgt die Erhebung und/ oder die Verarbeitung im Ausland, dann gilt nun *contrario* ausdrücklich überhaupt keine gesetzliche Bindung? Wenn auf Grundlage der bisherigen Gesetzeslage der Anwendungsbereich des BNDG im besten Fall wegen einer fehlender Klarstellung im Gesetz nur generell in Frage gestellt werden konnte, so ergeben sich jetzt, durch die pauschale Abgrenzung der Anwendungsbereiche, erhebliche Zweifel an eben jenen. Und das obwohl immer wieder betont wird, dass die Anwendbarkeit der Grundrechte gerade nicht auf das Bundesgebiet zu beschränken ist. Wäre ich nichtdeutscher Staatsbürger und hielte mich in Dänemark auf, so wäre es doch gleichgültig, ob der BND meine Daten erfasst, während er in Deutschland, neben mir in Dänemark oder in Indien sitzt.

Der BND darf nach § 3a Nr. 1- 3 des Gesetzentwurfs personenbezogene Daten aus internationalen Telekommunikationsnetzen erheben und verarbeiten, wenn dies erforderlich ist, um frühzeitig Gefahren für die innere und äußere Sicherheit der Bundesrepublik Deutschland zu erkennen und zu begegnen, ihre Handlungsfähigkeit zu wahren oder sonstige Erkenntnisse von {erheblicher} außen- oder sicherheitspolitischer Bedeutung zu gewinnen – mit anderen Worten: Durch die Zweckbindung erfolgt jedenfalls kaum eine effektive Begrenzung der Tätigkeit. Dass

diese weit formulierten Zwecke zu einem unverhältnismäßigen Eingriff insbesondere in Artikel 10 GG führen können, gibt das Gesetz selbst zu erkennen, indem es die Betroffenen in drei Klassen unterteilt: Die Daten von deutschen Staatsangehörigen dürfen überhaupt nicht in dieser Form, die von EU-Staatsangehörigen nur mit beschränkten Selektoren und die aller anderen umfassend erhoben werden. Wie das vor dem Hintergrund von Jedermann-Grundrechten und Diskriminierungsverboten funktioniert, bleibt ein weiteres Geheimnis.

Unsere Spekulationen über einen bestehenden oder nicht bestehenden Ring-Tausch von Daten wurden beseitigt, aber unsere Sorgen bleiben bestehen: In den § 3g ff. des Gesetzesentwurfs werden Kooperationsmöglichkeiten mit ausländischen Geheimdiensten formuliert und ausgeformt: Das Tauschen kann nun offiziell, ohne besondere Voraussetzungen und Einschränkungen, beginnen (oder fortgeführt werden).

Vollkommen ignoriert wurde im Zusammenhang mit außen- und sicherheitspolitischen Aktivitäten der Exekutive das Urteil des BVerfG vom 20. April 2016. Auch wenn das Urteil das Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (BKAG) betrifft, so enthält es doch verallgemeinerungsfähige Aussagen für jede Übertragung personenbezogener Daten. Bei der Beurteilung der Verfassungsmäßigkeit einer Übertragung an eine ausländische Stelle sei zwar die Eigenständigkeit der ausländischen Rechtsordnung zu achten, so dass kein gleichwertiger Schutz im Empfängerstaat gefordert wird. Anders als in den vorherigen Entscheidungen geht das BVerfG hier in Bezug auf Menschenrechtsverletzungen, die durch die Übertragung der Daten ermöglicht werden, aber einen Schritt weiter und schränkt den exekutiven Einschätzungsspielraum drastisch ein. Ob die Daten im Empfängerstaat zu politischer Verfolgung oder unmenschlicher Behandlung oder erniedrigender Bestrafung oder Behandlung genutzt werden, unterliege nicht der politischen Einschätzungsprärogative, sondern müsse sich auf Informationen stützen, die durch Datenschutzbeauftragte und Gerichte überprüfbar sind. Außerdem bedürfe es konkreter Absicherungen, sobald der Gesamteindruck eines menschenrechtlich angemessenen Umgangs mit den Daten erschüttert sei. Der Gesetzesentwurf enthält diesbezüglich lediglich die Anforderung, dass der Empfänger in einer Absichtserklärung die Zweckbindung zusichert und dass sich die ausländische öffentliche Stelle bereit erklärt, auf Ersuchen des BND Auskunft über die vorgenommene Verwendung der Daten zu erteilen. Präventive Einschränkungen und Zusicherungen, wie sie das BVerfG kürzlich forderte und die als einzige effektiven Schutz für die Betroffenen bewirken können, werden nicht aufgegriffen. Ebenso wenig bewirkt die Möglichkeit des BND, Auskunft über die Verwendung der Daten zu erhalten, für sich noch nicht, dass diese auch wahrgenommen wird. Eine Verpflichtung zur Überprüfung fehlt – Wegsehen ist ausdrücklich erlaubt.

Keine Utopie

Durch diese Kritikpunkte soll nicht die Utopie eines gläsernen Nachrichtendienstes herbeigeredet werden. Natürlich muss ein fähiger Auslandsnachrichtendienst

im Geheimen, grundsätzlich überall, wo Gefahren bestehen können, und ohne vorherige Zustimmung Dritter agieren können.

Diese Kritikpunkte sollen vielmehr aufzeigen, dass es in unserer Zeit aus menschen- und grundrechtlicher Perspektive nicht ausreicht, national und einzelstaatlich Eingriffsbefugnisse zu formulieren; dass es nicht ausreicht, einem Nachrichtendienst, der aus einer Umgebung stammt, in der kein Internet die Datenfülle unüberschaubar und unzugänglich machte, lediglich die Ziele seiner Überwachungstätigkeiten vorzuschreiben. Die Grundrechte, insbesondere das Grundrecht auf informationelle Selbstbestimmung und die Telekommunikationsfreiheit, können die dahinterstehende autonome Persönlichkeitsentwicklung nur dann schützen, wenn der Gesetzgeber sich bei der Ausformulierung an den bestehenden und zukünftigen Gefahren für diese orientiert. Anstelle also an den Handlungsort anzuknüpfen, muss über die nationalen Grenzen hinausgedacht werden – denn Daten orientieren sich auch nicht an nationalen Grenzen. Anstelle auf den Verbleib eines Datums bei einem einzelnen Nachrichtendienst abzustellen, muss an die Verwendungsmöglichkeiten und Übertragungsmöglichkeiten gedacht werden – denn diese können bei den unüberschaubaren Datenmengen nicht mehr kontrolliert und eingeschränkt werden.

Dabei kommt es auch darauf an, nach der Übertragung für die Verwendung durch den Empfänger verantwortlich zu bleiben – die Verwendung zu gezielten Tötungen im Rahmen der US-amerikanischen und britischen Drohneneinsätze ist zwar nur sehr schwer vorherzusehen oder nachzuweisen. Aber trotzdem besteht sie als reale Möglichkeit und es gibt viele [Anzeichen](#), die diese Verwendungen andeuten.

Angesichts der Datenmassen sollte auf der anderen Seite vermehrt darauf geachtet werden, die Effektivität der nachrichtendienstlichen Arbeit zu verbessern – nur eine Masse von Daten bedeutet nicht, dass auch die wesentlichen Daten gefunden werden, schon gar nicht in einem Bereich, in dem noch nicht im Vorhinein definiert sein kann, wonach überhaupt zu suchen ist.

